Получено выражение для расчета пропускной способности квантового канала связи, в котором передача информации осуществляется отдельными фотонами с двоичным кодированием символов «0» и «1» ортогональными поляризационными состояниями фотонов, с учетом вероятности деполяризации фотонов.

В работе установлены зависимости пропускной способности C_{max} от вероятности деполяризации фотонов p и от длины световода l. Получено, что с увеличением p от 0 до 0,5 пропускная способность квантового канала связи уменьшается. Аналогичные тенденции изменения имеет зависимость $C_{max}(l)$ на всем исследуемом диапазоне изменения l.

На основании выполненных экспериментальных исследований установлено, что для достижения максимальной пропускной способности рассматриваемого канала связи необходимо выбирать напряжение питания ЛФП, соответствующее наибольшей квантовой эффективности регистрации приемного модуля.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор №Т13-018).

Литература

1. *Килин С.Я., Хорошко Д.Б., Низовцев А.П. и др.* Квантовая криптография: идеи и практика. Минск, 2007.

ГЕНЕРАТОР АКУСТИЧЕСКОГО ШУМА С МИКРОПРОЦЕССОРНЫМ УПРАВЛЕНИЕМ

А.А. КАЗЕКА, В.А. ПОПОВ, М.А. ГОТОВКО

Защита от утечки информации по акустическому каналу возможно путем применения активных средств защиты, к которым относятся генераторы акустического шума. В настоящие время согласно нормативным требованиям применяются аналоговые генераторы акустического шума, построенные на базе источников случайных электрических колебаний типа «белый» шум.

В предложенном устройстве применяется до четырех независимых каналов, формирующих акустические шумовые сигналы. Каждый канал использует аналоговый генератор «белого шума» на базе полупроводникового диода, что позволяет получить не повторяющийся маскирующий сигнал в полосе частот от 160 Гц до 8000 Гц. На один канал возможно подключение до 30 акустических и виброакустических преобразователей. Отличительной особенностью данного устройства является микропроцессорное управление каналами генератора шума. Микропроцессор в зависимости от уровня речевого сигнала в защищаемом помещении автоматически изменяется уровень шумового сигнала в канале, что повышает защищенность речевого сигнала. Также предусмотрена цифровая регулировка уровней сигнала на верхних и нижних частотах, чувствительности встроенного и выносного микрофона и уровня шума в каждом канале, что позволяет проводить более точную настройку данного устройства на стадии его ввода в эксплуатацию. Кроме того, во время работы анализируется сигнал в каналах зашумления и в случае аварии срабатывает звуковая сигнализация, одновременно выводя на световой индикатор информацию о неисправности.

Таким образом, применение современной элементной базы в генераторе акустического шума позволило расширить его возможности, повысить надежность и удобство в эксплуатации.

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ЭЛЕКТРОМАГНИТНЫМ КАНАЛАМ

А.А. ЗИНЧЕНКО

Защита информации от утечки по электромагнитным каналам — это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода

конфиденциальной информации за пределы контролируемой зоны за счёт электромагнитных полей побочного характера и наводок.

Экранирование позволяет защитить от нежелательных воздействий электромагнитных сигналов и излучений собственных электромагнитных полей, а также ослабить или исключить паразитное влияние внешних излучений.

Электростатическое экранирование заключается в замыкании силовых линий электростатического поля источника на поверхность экрана и отводе наведённых зарядов на массу и на землю. Такое экранирование эффективно для устранения ёмкостных паразитных связей. Экранирующий эффект максимален на постоянном токе и с повышением частоты снижается.

Магнитостатическое экранирование основано на замыкании силовых линий магнитного поля источника в толще экрана, обладающего малым магнитным сопротивлением для постоянного тока в области низких частот. Электромагнитное экранирование ослабляет поле образующимися в толще экрана вихревыми токами. Заземление аппаратуры и её элементов используются для отвода наведённых сигналов на землю. Фильтрация применяется для подавления или ослабления сигналов при их возникновении или распространении, а также для защиты систем питания аппаратуры обработки информации.

Развязка представляет собой разделение различных электрических цепей с помощью специальных схем.

СОЗДАНИЕ МОДЕЛИ БЕЗОПАСНОСТИ ДЛЯ СОВРЕМЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

А.С. ПОТЕТЕНКО

Центры обработки данных (ЦОД) привлекают внимание многих злоумышленников. Исходя из анализа современных угроз безопасности информации, хранимой и обрабатываемой в ЦОД, для создания устойчивой модели безопасности необходимо предпринять следующие меры:

– определить зоны безопасности и установить для каждой из них уровни безопасности;

– провести оценку текущей ситуации в сфере безопасности для выявления уязвимостей и рисков нарушения безопасности;

–внедрить сетевую систему обнаружения вторжений для важных сетевых сегментов.

– ввести контроль межзонального доступа с использованием межсетевых экранов и маршрутизаторов;

– установить ограничения доступа, путем внедрения VLAN на уровне маршрутизаторов.

Принять меры по защите сети хранения данных выполнением следующих пунктов:

– защита сети хранения данных от внешних угроз, таких как атаки злоумышленников;

– защита сети хранения данных от внутренних угроз, таких как несанкционированный доступ сотрудников или доступ с использованием взломанных устройств;

– защита сети хранения данных от непреднамеренных угроз нарушения безопасности со стороны авторизованных пользователей, таких как неправильная конфигурация или ошибка пользователя;

– защита и изоляция среды каждого хранилища данных от других, даже если они находятся в пределах одной физической сети.

Внедрить средства эффективного управления и мониторинга для поиска и устранения неисправностей компонентов системы, обеспечения безопасности и функций программного обеспечения.